DATASHEET

Cynamics AI in the Edge and NVIDIA

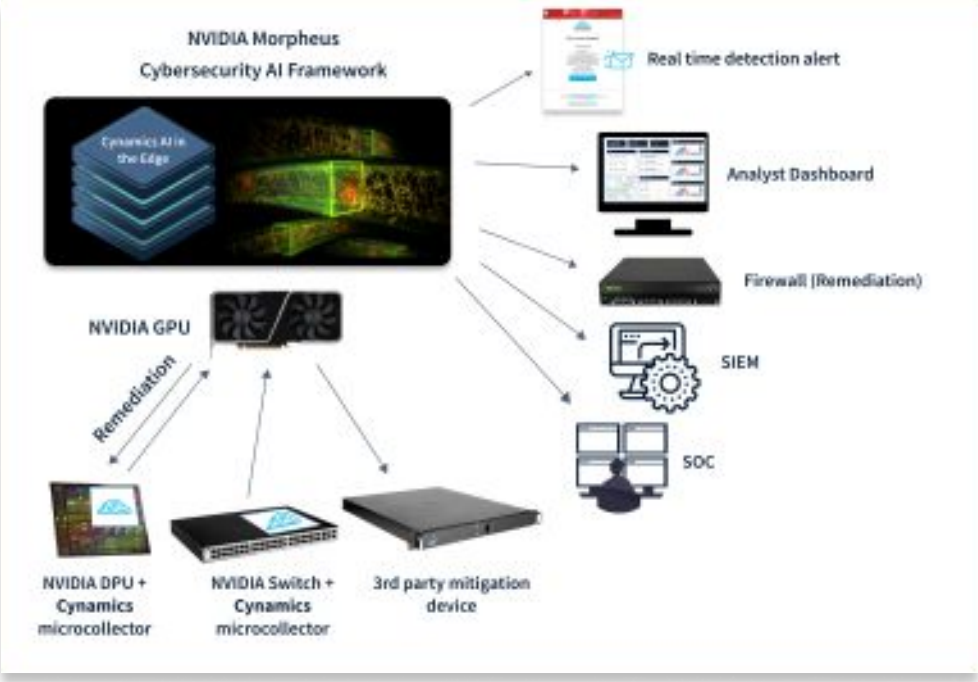
Full network protection for the largest and most complex networks

The future of Network Detection and Response (NDR) is total interoperability. Protection, detection, prediction – anywhere, anytime, with anything.
Cynamics next-gen NDR solution collects less than 1% of network traffic samples using standard sampling protocols and APIs built into every network gateway (physical or virtual, legacy or cloud), and provides complete 100% network coverage and protection at speed and scale with patented AI and ML algorithms. The solution is fully enterprise ready and deployed in hundreds of networks of all sizes and architectures.

Powered by a dedicated patent for crunching the small samples to ensure no network performance overheads, the Cynamics and NVIDIA collaboration is the only NDR solution that can work in the largest and most complex networks and data centers, any size, and any architecture. By combining NVIDIA Switches and DPUs with Cynamics AI, the largest networks can have full end-to-end coverage (100%) for the first time from less than 1% of network samples and mitigate threats long before they hit.

Once an attack is detected, full root-cause details of the threat are provided, and are automatically mitigated with Cynamics auto-remediation that sends instructions directly to the NVIDIA platforms and 3rd party integrations (e.g., Firewalls).

With this advanced technology at their fingertips, enterprises, government organizations, and data centers can be confident in protecting their networks from any threat.



The Cynamics Value

Granular Visibility

Covers your complete network across on-premise, cloud, and hybrid network environments to ensure full visibility from 1% samples

Eliminate Blind Spots

Spotlight hidden threats, identify suspicious behaviors, mitigate ongoing attacks and stop nefarious activity before it impacts operations

Expose Backdoors

Identifies vulnerabilities, intercepts malicious activity, and fortifies weak spots to keep attackers out and enable rapid remediation

Advanced Detection

Digests traffic behavior at every timestamp, comparing historical values and trends to detect suspicious patterns and reduces investigation time

Threat Prediction

AI technology which autonomously learns and discovers hidden patterns preceding attacks, based on normalizing all networks to create a global network blueprint

No Overhead

A dedicated patent for crunching the small samples to ensure no network performance overheads